IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN RE: BPS DIRECT, LLC and CABELA'S, LLC, WIRETAPPING	**MDL NO. 3074** **2:23-md-03074-MAK**

DEFENDANTS' MEMORANDUM IN SUPPORT OF THEIR MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Rules

INTRODUCTION

This putative class action consolidates multiple, virtually identical, class action complaints Plaintiffs filed across the country challenging Defendants' use of routine software-based solutions that improve the design, functionality, and user experience of their customer-facing website. Plaintiffs claim that the routine software BPS and Cabela's use to, for example, identify, troubleshoot, and remediate bugs on its website constitute "wiretapping," under the federal wiretap statute and the laws of five different states, and violates both state and federal law in other ways. Courts around the country have repeatedly and routinely reject claims just like these. Plaintiffs lack standing and Plaintiffs' Consolidated Class Action Complaint ("Complaint" or "Compl.") (ECF No. 53) fails on its face, demanding dismissal under either Rule 12(b)(1) or 12(b)(6).

FACTUAL BACKGROUND

Plaintiffs each allege that they visited the website of Cabela's and/or BPS. Some Plaintiffs allege that they made purchases from the websites (Compl. ¶104, 117), while others do not allege they made any purchase. Plaintiffs offer few specifics about their interactions with Defendants' websites; instead, alleging that Defendants generally procured third-party vendors "to embed snippets of JavaScript computer code . . . on Defendants' Websites." *Id.* ¶ 1. This code allegedly tracked their "mouse clicks and movements, keystrokes, search terms, substantive information inputted by Plaintiff[s], pages and content viewed by Plaintiff[s], scroll movement, and copy and paste actions." *E.g.*, *Id.* ¶¶ 99. In other words, Plaintiffs allege that Defendants use software code with a session replay feature to be able to reproduce a user's online experience to understand how visitors interact with the website. *Id.* ¶ 70. Nowhere do Plaintiffs allege that they were harmed by the use or purported use of this technology, beyond conclusory assertions of mental distress.

The lack of harm is unsurprising. Session replay software is a common analytics tool employed by numerous websites, including major retailers nationwide to ensure functionality on

their websites. It allows website owners to see if a technical issue is interfering with a user's desired website access. For example, repeatedly clicking a button on a website may indicate that the button is not operating correctly and requires maintenance. A website owner can enable session replay by embedding JavaScript code, provided by a session replay vendor, in the target website. The JavaScript code tracks specific browser events that occur on that website, such as mouse movements, clicks, scrolls, window resizing, and page loads. These discrete pieces of data are pieced together using session replay software to recreate a visual depiction of a user's website experience without exposing customers' personal information. In short, session replay simply "achieve[s] an improved technological result in *conventional industry practice.*" *Content Square SAS v. Quantum Metric, Inc.*, 2021 U.S. Dist. LEXIS 51656, at *13 (D. Del. Mar. 18, 2021).[1]

Undeterred, Plaintiffs assert sixteen counts: violation of the Federal Wiretap Act; violation of the Computer Fraud and Abuse Act ("CFAA"); violation of the California Invasion of Privacy Act ("CIPA"); statutory larceny; violation of California's Unfair Competition Law ("UCL"); violation of the Maryland Wiretapping and Electronic Surveillance Act; invasion of privacy under Maryland law; violation of the Massachusetts Wiretapping Statute; invasion of privacy (under Massachusetts law); violation of the Missouri Wiretap Act, violation of the Missouri Merchandising Practices Act, invasion of privacy (under Missouri law); violation of the Pennsylvania Wiretapping and Electronic Surveillance Control Act; invasion of privacy (under Pennsylvania law); trespass to chattels, and conversion to chattels.[2]

[1] Emphasis added throughout unless otherwise noted.

[2] While Defendants list Plaintiffs' sixteen counts here in the order that Plaintiffs plead them, as the Court noted in the initial case management conference, many of Plaintiffs' claims have similarities that require similar analyses. Accordingly, and in an attempt to most efficiently frame Plaintiffs' sprawling assortment of claims, Defendants' motion will address the claims by grouping similar Counts together.

LEGAL STANDARD

To survive a Rule 12(b)(1) motion to dismiss, Plaintiffs, as the party invoking federal jurisdiction, bear the burden of establishing the elements of standing, including injury in fact. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). To establish an injury in fact, Plaintiffs must show that they "suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Id.* at 339.

To survive a Rule 12(b)(6) motion to dismiss, a complaint's "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Bell Atl. Corp. v. Twombly,* 550 U.S. 544, 555 (2007). A complaint does not suffice if it tenders naked assertions devoid of further factual enhancement. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Rather, the complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face. *Id.* This demands "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 570.

ARGUMENT

I. Plaintiffs Lack Article III Standing.

Plaintiffs Complaint must be dismissed because Plaintiffs do not allege any concrete injury that confers Article III standing.

First, Plaintiffs' allegations that Defendants violated various statutes (Compl. ¶¶ 38-52) do not establish an injury in fact for Article III standing. Article III requires that a plaintiff's injury in fact "be 'concrete'—that is, 'real, and not abstract.'" *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021). This is true "even in the context of a statutory violation." *Id.* at 2205.

Plaintiffs do not meet their burden because they do not adequately plead they have suffered a concrete harm resulting from their visits to Defendants' websites. Courts in the Third Circuit and elsewhere reached this very conclusion in nearly identical circumstances. *See Cook v. Gamestop*,

2023 WL 5529772 at *2-6 (W.D. Pa. Aug. 28, 2023); *Massie v. General Motors LLC*, 2022 WL 534468 (D. Del. Feb. 17, 2022); *see also, e.g.*, *Mikulsky v. Noom, Inc.*, 2023 WL 4567096, at *6 (S.D. Cal. July 17, 2023) (dismissing for lack of standing because conclusory allegation that personal information was disclosed through defendant's use of session replay code "is insufficient to establish that [plaintiff] suffered a concrete harm").

Those courts have explained that, as is the case here, an alleged invasion of privacy is not sufficient to confer Article III standing when any information that was allegedly disclosed was not sufficiently private. Here, at most, Plaintiffs Calvert, Durham[3], Hernandez, Moore, Tucker, and Vonbergen (who do not allege to have even purchased anything from Defendants' websites) allege that Defendants' websites captured her browsing activity on a public website. That information is not personal or private and does not give rise to Article III standing. *See Cook*, 2023 WL 5529772 at *5 (dismissing claims based on session replay software for lack of standing and stating that nearly identical information "is no different from what [defendant's] employees would have been able to observe if [plaintiff] had gone into a brick-and-mortar store and began browsing the inventory"); *Lightoller v. JetBlue Airways Corp.*, 2023 WL 3963823, at *4 (S.D. Cal. June 12, 2023) (dismissing session replay case for lack of standing where only information allegedly disclosed related to browsing for flight information); *Massie*, 2022 WL 534468 at *5 ("'Eavesdropping' on communications that do not involve personal information, personally identifiable information, or information over which a party has a reasonable expectation of privacy does not amount to a concrete injury"). Plaintiffs Cornell and Montecalvo fare no better; though they allege that they made purchases from Defendants' websites, thus providing the basic personal

[3] As to Plaintiff Durham, the Complaint is *entirely* devoid of any specific allegations beyond Plaintiff Durham's citizenship. Compl. ¶ 12.

information needed to make an online purchase. Compl. ¶¶ 104, 117. Disclosure of basic personal information likewise does not give rise to Article III standing. *See I.C. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049-50 (N.D. Cal. 2022) (finding disclosure of "basic contact information, including one's email address, phone number, or . . . username" inadequate to establish standing); *Brignola v. Home Properties, L.P.*, 2013 WL 1795336, at *12 (E.D. Pa. Apr. 26, 2013) (finding that a plaintiff's "name, address, phone number, etc. . . . are not private facts actionable for an [invasion of privacy] claim"). Plaintiffs' allegations of bare statutory violations do not confer standing.

Second, Plaintiffs' threadbare assertions that Defendants' conduct caused Plaintiffs "mental anguish and suffering" (Compl. ¶ 290) and the "diminution of the value of their private and personally identifiable data and content" (Compl. ¶ 246) are the exact type of conclusory allegations that courts must disregard on a motion to dismiss. *See Lasche v. New Jersey*, 2022 WL 604025, at *3 (3d Cir. Mar. 1, 2022) (instructing courts considering a motion to dismiss to disregard threadbare and speculative allegations). Moreover, even if supported by actual facts, these theories of damage are often rejected by courts as insufficient to confer standing. *See, e.g.*, *Kury v. Abbott Lab'ys, Inc.*, 2012 WL 124026 (D.N.J. Jan. 17, 2012) (finding conclusory claims of mental anguish insufficient); *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 755 (W.D.N.Y. 2017) ("Courts have routinely rejected the proposition that an individual's personal identifying information has an independent monetary value"). These conclusory allegations of damages do not confer standing.

II. Alternatively, Plaintiffs Lack Standing to Assert Claims for Injunctive Relief

Plaintiffs lack standing to seek an injunction. An injunction is only appropriate to protect against future harm. Here, Plaintiffs do not, *and cannot*, allege that they will visit basspro.com or cabelas.com without knowledge that the sites employ session replay. Indeed, Plaintiffs are clearly aware of the use of session replay on the website, and any future visit to the websites will be made

with such knowledge. Because Plaintiffs cannot contend that they will suffer the future harm of visiting Defendants' websites with session replay running without their knowledge, they lack standing to pursue a claim for injunctive relief. *See, e.g.*, *In re Johnson & Johnson Talcum Powder Prod. Mktg., Sales Pracs. & Liab. Litig.*, 903 F.3d 278, 292-93 (3d Cir. 2018) (finding that "[t]he law affords [the plaintiff] the dignity of assuming that she acts rationally, and that she will not act in such a way that she will again suffer the same alleged 'injury.'"); *Winkworth v. Spectrum Brands, Inc.*, 2020 WL 3574687, at *8 (W.D. Pa. June 30, 2020) (similar); *McNair v. Synapse Grp. Inc.*, 672 F.3d 213, 224 (3d Cir. 2012) (concluding former customers lacked standing to pursue injunctive relief in the absence of allegations that they intended to subscribe for magazines through the same marketer). Even in data breach cases, courts routinely deny declaratory relief involving past cyberattacks because it "will not provide any relief for past injuries or injuries incurred in the future because of a data breach that has already occurred." *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *8 (S.D. Cal. Nov. 3, 2016).[4] Plaintiffs' claims for injunctive relief should therefore be dismissed.

III. Plaintiffs' Various Wiretap Claims (Counts I, III, VI, VIII, X, and XIII) Fail.

Plaintiffs assert claims (Counts I, III, VI, VIII, X, and XIII) under six different state and federal statutes directed at wiretapping: the Federal Electronic Communications and Privacy Act, and the analogous state statutes from California, Maryland, Massachusetts, Missouri, and Pennsylvania. Each of these claims fails for a number of independent reasons.[5]

[4] *See also, e.g.*, *Kuhns v. Scottrade, Inc.*, 868 F. 3d 711, 718 (8th Cir. 2017) (same); *Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1073 (C.D. Ill. 2016) (same).

[5] For convenience, Defendants have attached a chart indicating which of the following arguments apply to which wiretap statutes as Appendix 1.

a. Defendants' Consent and/or Party Status Preclude Claims Under the Federal, California, and Missouri Acts (Counts I, III, and X)

It is undisputed that Defendants were parties to the alleged communication who allegedly caused any recording to occur, did consent to the interception. This dooms Plaintiffs' wiretap claims under the federal, California, and Missouri statutes.

i. Defendants were parties to the allegedly intercepted communications.

The federal and Missouri statutes expressly state that "a party to the communication" cannot be liable for wiretapping or eavesdropping. 18 U.S.C. § 2511(2)(d) ("it shall not be unlawful under this chapter for a person…to intercept a wire, oral, or electronic communication where such person is a party to the communication."); MO. STAT. § 542.402.2(3) (same); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 607 (9th Cir. 2020) (noting that the federal Wiretap Act "contain[s] an exemption from liability for a person who is a 'party' to the communication . . ."); *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 143 (3d Cir. 2015) (same).)

Similarly, Plaintiffs cannot maintain a claim against Defendants pursuant to the California act because the statute does not prohibit a party to the communication from recording it. "Section 631 was aimed at one aspect of the privacy problem—eavesdropping, or the secret monitoring of conversations by third parties." *Ribas v. Clark*, 38 Cal. 3d 355 at 359 (1985) (citing *Rogers v. Ulrich*, 52 Cal. App. 3d 894, 899 (1975).) "Only a third party can listen to a conversation secretly . . . . By contrast, a party to a communication can record it (and is not eavesdropping when it does)." *Graham*, 533 F. Supp. 3d at 831 (*citing Rogers*, 52 Cal. App. 3d at 897-99); *see also, e.g.*, *Warden v. Kahn,* 99 Cal. App. 3d 805, 811 (Ct. App. 1979) (Section 631 "has been held to apply only to eavesdropping by a third party and not to recording by a participant to a conversation.").

As the intended recipient of Plaintiffs' communications, there is no question that Defendants were a party to the communications. *See Jurgens v. Build.com, Inc.*, 2017 WL 5277679, at *5 (E.D. Mo. Nov. 13, 2017) ("[T]he intended recipient of such transmission is a party to the communication" (*citing In re Google*, 806 F.3d at 143 (3d Cir. 2015))). Plaintiffs admit as much in the Complaint. *See* Compl. ¶ 238 ("Plaintiffs and the California Subclass Members interacted with Defendants' Websites reasonably believing that their browsing activities—and any facts and information *communicated to Defendants' Websites*—were secure and confidential (i.e., solely *between themselves and Defendants*")).

ii. Defendants consented to any alleged interception.

Under the federal and Missouri wiretap acts it is not unlawful to intercept a communication "where one of the parties to the communication has given prior consent to such interception[.]" 18 U.S.C. § 2511(2)(d) ("it shall not be unlawful under this chapter for a person…to intercept a wire, oral, or electronic communication. . . where one of the parties to the communication has given prior consent to such interception."); MO. STAT. § 542.402.2(3) (same).

As the party allegedly responsible for the "interception," Defendants undoubtedly consented to the alleged conduct. And this fact alone is sufficient to dismiss Counts I and X under the one-party consent framework of the federal and Missouri laws. *See Phillips v. Am. Motorist Ins. Co.*, 996 S.W.2d 584, 589 (Mo. Ct. App. 1999) ("It is not unlawful for a person to intercept a communication to which he is a party or where one of the parties to the conversation has consented to the interception, provided that he is not doing so for a 'criminal or tortious' purpose.").

iii. Plaintiffs fail to allege a criminal or tortious purpose.

Plaintiffs allege that Defendants should nonetheless be held liable under the federal and Missouri laws because an exception to the exceptions in 18 U.S.C. § 2511 and MO. STAT. § 542.402.2(3) applies. Specifically, Plaintiffs contend Defendants intercepted Plaintiffs'

communications "for the purpose of committing [a] criminal or tortious act," namely invading Plaintiffs' privacy. Compl. ¶¶ 181, 359.

Courts interpreting the federal statute have consistently held that, "a plaintiff cannot establish that a defendant acted with a 'criminal or tortious' purpose simply by proving that the defendant committed any tort or crime." *In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d 497, 516 (S.D.N.Y. 2001) (The "criminal or tortious" requirement "is to be construed narrowly, covering only acts accompanied by a specific contemporary intention to commit a crime or tort."). This is because "the focus [the criminal or tortious requirement] is not upon whether the interception itself violated another law; it is upon whether the purpose for interception—*its intended use*—was criminal or tortious." *Id.* (emphasis supplied) (quoting *Sussman v. ABC*, 186 F.3d 1200, 1202–03 (9th Cir. 1999) ("Where the purpose is not illegal or tortious, but the means are, the victims must seek redress elsewhere.")).

In other words, "the commission of a tortious act [does] not prove a tortious purpose." *Id.* (citing *Desnick v. Am. Broad. Companies, Inc.*, 44 F.3d 1345, 1353 (7th Cir. 1995) ("The defendants did not order the camera-armed testers into the [defendants'] premises in order to commit a crime or tort. Maybe the program as it was eventually broadcast was tortious, . . . [b]ut there is no suggestion that the defendants sent the testers into the Wisconsin and Illinois offices for the purpose of defaming the plaintiffs"); *see also id.* (citing *Boddie v. ABC*, 881 F.2d 267, 270 (6th Cir. 1989) ("It is the use of the interception with intent to harm rather than the fact of interception that is critical to liability"); *Meredith v. Gavin*, 446 F.2d 794, 799 (8th Cir. 1971) ("[I]t seems apparent from the context in which the statute was enacted that the sort of conduct contemplated was an interception by a party to a conversation with an intent to use that interception against the non-consenting party in some harmful way and in a manner in which the offending

party had no right to proceed."); *Lucas v. Fox News Network, LLC*, 248 F.3d 1180 (11th Cir. 2001) ("Because the complaint does not allege that defendants intercepted a communication for the purpose of committing any criminal or tortious act, it fails to state a claim"); *Caro v. Weintraub*, 618 F.3d 94, 99–100 (2d Cir. 2010) ("At the time of the recording the offender must intend to use the recording to commit a criminal or tortious act.").

Thus, in order for an act to be done with a "criminal or tortious purpose," the offender must "plan[] to use the recording to harm the other party to the conversation[.]" *Caro*, 618 F.3d at 99–100. Indeed, "[i]ntent may not be inferred simply by demonstrating that the intentional act of recording itself constituted a tort. A simultaneous tort arising from the act of recording itself is insufficient." *Id.* As the Second Circuit noted, "Congress chose the word 'purpose' for a reason." *Caro*, 618 F.3d at 100. "Had Congress intended for the act of recording itself to provide the tortious intent necessary, it could have chosen to define the exception in terms of interception of oral communications resulting in a tortious or criminal act. But Congress limited the cause of action to instances where one party to the conversation deliberately seeks to harm the other participant through the information intercepted." *Id.*

Here, Plaintiffs' only basis for "tortious or criminal" intent is that Defendants allegedly acted with the intent to invade Plaintiffs' privacy in violation of common law and state wiretap statutes. *See* Compl. ¶¶ 181, 359. But even accepting this conclusory allegation as true, the Complaint does not allege that Defendants intended to use *the allegedly intercepted information* for a criminal or tortious purpose. Indeed, Plaintiffs repeatedly allege that Defendants' purpose for the allegedly intercepted information was to "use[] that data and information to maximize profits through predictive marketing and other targeted advertising practices." *E.g.*, Compl. ¶¶ 294, 337, 400, 439. Not only is this allegation conclusory, it also does not allege any criminal or tortious

conduct by Defendants, because it is not illegal to increase profit margins. At bottom, Plaintiffs' allegation is based entirely on the premise that because Defendants allegedly committed a tortious act, its intent must also be tortious. As discussed above, courts have repeatedly rejected this premise.

Counts I, III and X should be dismissed.

b. Plaintiffs do Not Allege Interception of any "Contents" Under the Federal, California, Maryland, Massachusetts, and Pennsylvania Acts

Plaintiffs further fail to state a viable claim under the federal, California, Maryland, Massachusetts, and Pennsylvania wiretap laws because Defendants have not acquired any "contents". Not all data related to the communications trigger these privacy statutes. Each statute only prohibits the unlawful interception of the "contents" of a communication. *See* 18 U.S.C. § 2510(8); Md. Code, Cts. & Jud. Proc. § 10-401(4); Mass. Gen. Laws ch. § 272; 18 Pa. C.S. § 5702.

The wiretap statutes define "contents" as "any information concerning the substance, purport, or meaning of [a] communication." *See, e.g.*, 18 U.S.C. § 2510(8).[6] In other words, the defendant must capture "the intended message conveyed by the communication," like the text of an email message or words spoken on a call. *Cook*, 2023 WL 5529772 at *6; *see also In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). Accordingly, types of information that Courts have found to constitute "contents" in the wiretapping context include passwords, instant messages, and text messages.[7] *See, e.g.*, *Rich v. Rich*, 2007 WL 4711508, at *3 (Mass. 2007)

[6] The Maryland statute also includes information concerning the "existence" of the communication. Md. Code, Cts & Jud. Proc. § 10-401(4). The Massachusetts statute also includes "information concerning identity of the parties." Mass. Gen. Laws ch § 272.

[7] A Massachusetts trial court recently found that data allegedly collected by session replay code could constitute "contents" under the Massachusetts act. *Alves v. BJ's Wholesale Club, Inc.*, 2023 WL 4456956 (Mass. Super. June 21, 2023). The *Alves* court's decision is not binding on this Court but, even to the extent the Court finds it persuasive, Plaintiffs' claim under the Massachusetts statute fails for other reasons discussed herein.

(finding "contents" to include passwords and instant messages); *Commonwealth v. Moody*, 466 Mass. 196, 207-209 (Mass. 2013) (finding text messages are held to be covered by the Wiretap Statute). These "contents" can be distinguished from "non-content" or "record information" about a communication, like "extrinsic information used to route a communication," that is not actionable if collected. (*In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 135 (3d Cir. 2015); *In re Zynga Priv. Litig.*, 750 F.3d at 1108.

"Contents" does *not* include "dialing, routing, addressing, or signaling" information, such as "addresses, phone numbers, and URLs . . . when they are performing such a function." *In re Google*, 806 F.3d at 137. Plaintiffs assert generally that Defendants captured website visitors' mouse movements, clicks, keystrokes, and URLs of web pages visited, though they do not allege their own interactions with the websites with any level of factual specificity. Compl. ¶¶ 1, 68. Even if sufficiently pled though, that information does not constitute "contents."

Mouse movements, clicks, and keystrokes are not "contents" of a communication because they disclose only location information; in fact, such information is not even a communication at all. Similar to a visitor's physical movements recorded through video surveillance at a brick-and-mortar store, a visitor's "movements" on Defendants' websites are not "contents" because they "d[o] not convey the substance of any particular communication." *Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318, 1321–22 (S.D. Fla. 2021) (applying the same analogy and holding mouse movements, clicks, pages visited, and keystrokes, including information allegedly input by the plaintiff, were not "contents" under Florida's wiretap statute); *see also, e.g.*, *Cook* 2023 WL 5529772 at *8; *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021) (dismissing plaintiff's wiretapping claim based on session replay "to the extent that it is predicated on non-content information"); *Jacome*, 2021 WL 3087860, at *4 (dismissing plaintiff's wiretapping claim

based on the same data because it "is precisely the type of non-record information that courts consistently find do not constitute 'contents' under the Federal Wiretap Act or any of its state analogs because it does not convey the substance or meaning of any message," and collecting cases); *Cardoso v. Whirlpool Corp.*, 2021 WL 2820822, at *2 (S.D. Fla. July 6, 2021) (finding *Jacome* "persuasive" and adopting its reasoning).[8]

Nor are URLs "contents" under the wiretap statutes. A URL is a Uniform Resource Location, a "file path" to take a webpage visitor to a particular location, *i.e.*, a "file contained in a folder on a web server owned or operated by [the defendant]" "used to identify the physical location of documents on servers connected to the internet." *In re Nickelodeon Consumer Priv. Litig.*, 2014 WL 3012873, at *15 (D.N.J. July 2, 2014) (internal quotation marks omitted). This data plainly reflects a "dialing, routing, addressing, or signaling" function, not the substance written in a communication. *In re Google*, 806 F.3d at 137. As courts have found, a URL has "less in common with 'the spoken words of a telephone call,' than [it] do[es] with the telephone number dialed to initiate the call," because they are "static descriptions more akin to 'identification and address information.'" *In re Nickelodeon*, 2014 WL 3012873, at *15 (rejecting any argument that a URL was a "contents" for wiretapping purposes) (citations omitted)).

Put differently, "location identifiers," like URLs, "have classically been associated with non-content 'means of establishing communication.'" *In re Google*, 806 F.3d at 136. Capturing such non-communicative non-contents information does not violate wiretap statutes. *See, e.g.*, *Cook*, 2023 WL 5529772 at *9; *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082–83 (C.D. Cal. 2021) (clicks, pages visited, and keystrokes, including shipping and billing information,

[8] Under Florida's wiretapping statute, "contents," is defined, similarly to the wiretap statutes at issue here, as "includ[ing] any information concerning the substance, purport, or meaning of that communication." Fla. Stat. § 934.02.

are not "contents" for wiretapping purposes); *Bums v. Heyns*, 2015 WL 4391983, at *18 (W.D. Mich. July 15, 2015) (holding that clickstream data containing "the time, order and duration the computer spent on each web page as well as which files were accessed and/or downloaded . . . does not convey the 'substance, purport, or meaning' of a prisoner's communication").

Finally, Plaintiffs fail to allege that Defendants' session replay software captured "information concerning the identity of the parties to the communication" under the Massachusetts act. According to Plaintiffs, the identity of the website visitor *could potentially* be captured depending on the session replay software's configuration. *See* Compl. ¶¶ 75-80. But Plaintiffs fail to allege that Defendants' software had that ability to capture identifying information, or that it actually did so. At most, Plaintiffs allege that Defendants' session replay software collected "basic information about website user *sessions, interactions, and engagement*, with the capacity to break down users by device type, location, and [unidentified] other dimensions." Compl. ¶ 90. Plaintiffs' vague allegations about what *could* have been captured are insufficient to state a claim.

Based on the foregoing, because Plaintiffs have failed to allege that any contents have been intercepted by Defendants, Counts I, III, VI, VIII, and XIII should be dismissed.

c. Plaintiffs Do Not Allege a Contemporaneous "Interception" Under the Federal, California, and Maryland Acts

To "intercept" a communication under the federal, California, and Maryland, statutes, the acquisition must occur contemporaneous with the transmission of the messages. *Martin v. State*, 96 A.3d 765, 776 (Md. Ct. App. 2014) (citation omitted) (adopting the contemporaneous requirement "[i]n light of the nearly identical definitions of 'intercept' and 'electronic communication' in both the Federal and Maryland Wiretap Acts"); *Konop v. Hawaiian Airlines, Inc.,* 302 F.3d. 868, 878 (9th Cir. 2002) (under the federal wiretap act, the interception of a communication "in transit" means it must be "acquired during transmission" and not after the

communication has already been received by the recipient and "is in electronic storage"); *NovelPoster v. Javitch Canfield Grp.,* 140 F. Supp. 3d 938, 953 (N.D. Cal. 2014) (applying *Konop's* analysis of the Wiretap Act to claim under the California act). Here, any alleged interception of Plaintiffs' interactions with Defendants' website did not occur contemporaneous to their transmission. Instead, the Complaint reveals that a user's interactions with Defendants' website are captured in intervals, "accumulated," and sent "in blocks periodically throughout the user's website session"—not contemporaneously. Compl. ¶ 68. For this independent reason, Plaintiffs' Counts I, III, and VI should be dismissed. *See, e.g.*, *Jacome v. Spirit Airlines*, 2021 WL 3087860, at *6 (Fla. Cir. Ct. June 17, 2021) (finding "allegations without pleading any ultimate facts in support are insufficient to demonstrate that any interception happened contemporaneously with transmission."); *Adler v. Community.com,* 2021 WL 4805435, at *4 (C.D. Cal. Aug. 2, 2021) (dismissing CIPA claim because plaintiff did not state a "plausible allegation that Defendant acted to learn the contents of the message while they were, in a technical sense, in transit or in the process of being received.").

d. Session Replay Software Is Not a "Device" Under the Maryland, Massachusetts, and Pennsylvania Acts

The Maryland, Massachusetts, and Pennsylvania acts only apply to specific, statutorily defined "devices" or "intercepting devices." Md. Code, Cts. & Jud. Proc. § 10-401(8) (defining "device" under the Maryland act as "any device or electronic communication."); Mass. Gen. Laws ch. 272 § 99(B)(3) (defining "intercepting device" under the Massachusetts law as "[a]ny device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication."); 18 Pa. C.S. § 5702 (defining "device" under Pennsylvania law as "[a]ny ***device*** or ***apparatus*** . . . that can be used to intercept a wire, electronic or oral communication.).

Plaintiffs allege that session replay code falls within the relevant definition of each of these statutes. Compl. ¶ 267, 309, 413. But software code on a website—which is all that session replay technology is—is not a covered device under any of these three acts.

Maryland: The Maryland statute defines a "device" as "any device or electronic communication." Md. Code, Cts. & Jud. Proc. § 10-401(8). Plaintiffs fail to allege that session replay software falls within either of these terms. Plaintiffs do not allege—and there are no facts in the Complaint to support—that session replay software is an "electronic communication." And session replay software is not a "device" either. Courts interpret these terms according to "the language's natural and ordinary meaning, by considering the express and implied purpose of the statute, and by employing basic principles of common sense, the meaning these words intend to convey." *See Schmerling v. Injured Workers' Ins. Fund*, 795 A.2d 715, 720 (Md. 2002). Under their plain and ordinary meanings, a "device" or "apparatus" must be tangible; a device does not encompass intangible software code on a website. *See* Black's Law Dictionary (11th ed. 2019) (defining "device" as "[a] mechanical invention that may be "an apparatus or an article of manufacture," and defining "apparatus" with reference to "machine," which is defined as "[a] device or apparatus consisting of fixed and moving parts").

Indeed, consistent with this plain meaning, Maryland courts have interpreted the term "device" to include only tangible equipment. *See Mason v. Mach. Zone, Inc.*, 140 F. Supp. 3d 457, 462–63 (D. Md. 2015), *aff'd*, 851 F.3d 315 (4th Cir. 2017) (interpreting a California law criminalizing the ownership of a "slot machine or device" as regulating "a piece of equipment," *i.e.*, something tangible); *Cavanaugh v. State*, 2020 WL 3485717, at *4 (Md. Ct. Spec. App. June 26, 2020) (finding that a cell phone used as a recording device was a "device"). Accordingly, Plaintiffs' claim under the Maryland act (Count VI) fails.

Massachusetts: The Massachusetts act defines an "intercepting device" as "[a]ny ***device*** or ***apparatus*** which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication." Mass. Gen. Laws ch. 272 § 99(B)(3). Interpreting the words of the statute according to "common and approved usage"—as required under Massachusetts law, Mass. Gen. Laws ch. 4 § 99(B)(3)—a "device" or "apparatus" must be tangible; it does not encompass intangible software code on a website. *See* Black's Law Dictionary (11th ed. 2019) (defining "device" as "[a] mechanical invention that may be "an apparatus or an article of manufacture," and defining "apparatus" with reference to "machine," which is defined as "[a] device or apparatus consisting of fixed and moving parts").

Pennsylvania: The Pennsylvania statute defines a "device" as "[a]ny ***device*** or ***apparatus*** . . . that can be used to intercept a wire, electronic or oral communication." 18 Pa. C.S. § 5702 (emphasis added). Interpreting the words of the statute according to "common and approved usage"—as required under Pennsylvania law, *see Commonwealth v. Hart*, 28 A.3d 898, 908 (Pa. 2011)—a "device" or "apparatus" must be tangible; it does not encompass intangible software code on a website. *See* Black's Law Dictionary (11th ed. 2019) (defining "device" as "[a] mechanical invention that may be "an apparatus or an article of manufacture," and defining "apparatus" with reference to "machine," which is defined as "[a] device or apparatus consisting of fixed and moving parts").

Indeed, consistent with the principles discussed above for each state, many courts have held that session replay and similar software are not a "device" or "apparatus" under similar wiretap laws. *See, e.g.*, *Potter v. Havlicek*, 2008 WL 2556723, at *8 (S.D. Ohio June 23, 2008) (dismissing federal wiretap claim because "the word 'device' does not encompass software"); *Jacome*, 2021 WL 3087860, at *5 (dismissing Florida wiretap claim because session replay

software is not a "device or apparatus"); *Cardoso v. Whirlpool Corp.*, No. 21-CV-60784-WPD, 2021 WL 2820822, at *2 (S.D. Fla. July 6, 2021) (same); *Connor v. Whirlpool Corp.*, 2021 WL 3076477, at *2 (S.D. Fla. July 6, 2021) (same); *cf. United States v. Ackies*, 918 F.3d 190, 199 n.5 (1st Cir. 2019) (rejecting argument that software is a "device" under Federal Stored Communications Act because "software is not a 'device' under its plain meaning"); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 972 (S.D. Cal. 2012) ("[S]oftware is not a tangible good or service.").

As session replay software is not tangible—it cannot be a "device" under the Maryland, Massachusetts, or Pennsylvania acts. Counts VI, VII, and XIII therefore should be dismissed.

e. Session Replay Software Falls within the "Telephone Exception" to the Maryland Act (Count VI)

Even if session replay software could be considered a "device," Plaintiff Hernandez's claim under the Maryland wiretap statute would still fail because, in that case, session replay software would fall squarely within the statute's "telephone exemption." As discussed above, the Maryland wiretap act only applies to "devices." *Schmerling v. Injured Workers' Ins. Fund*, 795 A.2d 715, 721 (Md. 2002). But the statute specifically excepts from its definition of "device" certain equipment or components thereof—like session replay software—used in a business's communications systems.

To satisfy the "telephone exemption," "(1) the equipment must be a telephone instrument, equipment or other facility for the transmission of electronic communications, or any component thereof; and (2) the equipment must be used in the ordinary course of the subscriber's or user's business." *Id.* at 728 (quotation marks omitted); *see also* Md. Code, Cts. & Jud. Proc. § 10-401(8). Session replay software easily satisfies both elements.

Despite its name, the "telephone exemption" extends to more than just telephones. Indeed, to qualify for this exemption, session replay software need only "further the use of or functionally enhance the []communications system." *Schmerling*, 795 A.2d at 726. It does so if it has "a positive impact on the efficiency, clarity, cost, or any other factor by which one would measure the effects on a communications system." *Id.* (citing *Pascale v. Carolina Freight Carriers Corp.*, 898 F. Supp. 276, 281 (D.N.J. 1995)); *see also Adams v. State*, 424 A.2d 344 (Md. 1981) (finding an extension phone, which "allow[s] anyone in the room to hear the communication," fits within the telephone exemption because it "increase[s] the ability of the phone equipment to accommodate more parties to the communication.").

This standard is easily satisfied here. Plaintiff Hernandez alleges that session replay software enables Defendants to "record, save, analyze and replay website visitors' interactions" with its website. Compl. ¶ 64. The collection of this information aids "web designers with detailed insights into the user behavior by intercepting and recording website visitors 'as they click, scroll, type or navigate across different web pages.'" *Id.* Session replay software allows Defendants to, for example, fix broken links caught by repeated mouse clicks, improve the layout of its website, and ensure online customers can quickly and efficiently find the products they are looking for. In other words, if Plaintiff Hernandez's theory is that website visits are communications between Defendants and their website visitors, session replay software simply helps Defendants communicate with their website visitors, and helps website visitors effectively communicate with Defendants. As a result, Defendants' session replay software furthers "the use of or functionally enhance[s] [Defendants'] telecommunications system." *Schmerling*, 795 A.2d at 726.

The facts here differ from *Schmerling*, where the court found that the defendant's phone monitoring system was not covered by the telephone exemption, because it did "not contribute to

the functionality of the phone system in that [it did] not relate to the facilitation of communication." *Id.* at 727. Here, however, session replay software contributes directly to the functionality of Defendants' website, as established by Plaintiff Hernandez's own allegations. As Plaintiff Hernandez alleges, the software is used for "legitimate purposes" including to allow "website designers" to gain "insights into the user experience" on Defendants' website, and it is used in the ordinary course of Defendants' business. Compl. ¶ 64. This Court should conclude that session replay software falls within the telephone exemption and dismiss Count VI of the Complaint.

f. Session Replay Data Is Not an "Electronic Communication" Under the Pennsylvania Act.

Plaintiffs' claim under the Pennsylvania Act fails for the additional reason that—even if Plaintiffs are correct and session replay code is a "device" under statute, then it is a tracking device. Excluded from the Act's definition of "Electronic communication" is "any communication from a tracking device," which is "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 Pa. Cons Stat. § 5702. What Plaintiffs define as "Website Communications" are actually her movements on Defendants' websites: "mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time." Compl. ¶ 1.

Thus, even if session replay software is a "device" (it is not), the Court should find that it is a "tracking device," and that Defendants have not intercepted an "electronic communication." As discussed *supra*, at least two courts considering Florida's parallel wiretap statute have held that mouse clicks and website commands relate solely to a plaintiff's virtual online movement and are therefore not communications. *Jacome*, 2021 WL 3087860, at *3 (finding software that "tracks a website browser's movements" is "definitionally excluded from the term "'electronic communications'"); *see also Goldstein*, 559 F. Supp. 3d at 1321 (dismissing wiretap claims

because the "mere tracking of Plaintiff's movements on Defendant's website is the cyber analog to record[ing] information Defendant could have obtained through a security camera at a brick-and-mortar store."). Ultimately, regardless of the Court's decision whether session replay software is a device, Plaintiffs have failed to state a claim under the Pennsylvania act and Count XIII should be dismissed.

g. Plaintiffs' Consent Bars All of Plaintiffs' Wiretap Claims.

Prior consent is a complete defense to any alleged interception under each of the wiretap statutes on which Plaintiffs premise their wiretap claims. *See* 28 U.S.C. § 2511(2)(d) ("It shall not be unlawful . . . to intercept a wire, oral, or electronic communication where . . . one of the parties to the communication has given *prior consent* to such interception."); Mo. Stat. § 542.402.2(3) (same); 18 Pa. Cons. Stat. § 5704(4) (same); Cal. Penal Code § 631(a); Mass Gen. Law ch 227, § 99(B)(4) (defining an interception under the Massachusetts act as to "*secretly* hear, *secretly* record); Md. Code, Cts. & Jud. Proc. § 10-402(c)(3) ("It is lawful under this subtitle for a person to intercept a . . . communication . . . where all of the parties to the communication have given *prior consent* to the interception"). Prior consent does not require actual knowledge by Plaintiffs that they were being recorded—rather, as long as there is evidence that "the person being recorded 'knew or should have known, that the conversation was being recorded'" and proceeded to make the communication, the person is deemed to have consented by conduct. *Commonwealth v. Byrd*, 235 A.3d 311, 319 (Pa. 2020); *see also Silver v. Stripe, Inc.*, 2021 WL 3191752 at *4 (N.D. Cal. July 28, 2021) ("Courts consistently hold that terms of service and privacy policies . . . can establish consent to the alleged conduct challenged under various states wiretapping statutes and related claims"); *see also, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 2013 WL 5423918 at *12-13 (N.D. Cal. Sept. 26, 2013) (recognizing consent under federal and California acts can be express or implied). Here, any reasonable person would have known or

reasonably known that their website activities could be captured—indeed, Defendants' publicly available privacy statements made as much clear to Plaintiffs, just like all of its website users.

Specifically, Defendants notify their website users via their publicly posted privacy statements that they "may use third party-placed tracking pixels and Cookies and related or similar technologies to help us understand how to improve the customer experience on our Sites, to personalize our content, and to develop and improve our products and services, including advertising." BPS's Privacy and Security Statement, https://www.basspro.com/shop/en/privacy-policy-summary-bass-pro-shops (the "BPS Privacy Statement")[9]; *see also* Cabela's Privacy and Security Statement, https://www.cabelas.com/shop/en/privacy-policy-summary-cabelas (last visited Aug. 25, 2023)[10] (Cabela's "may use third party-placed tracking pixels and Cookies and related or similar technologies to help us understand how to improve the customer experience on our Sites, to personalize our content, and to develop and improve our products and services, including advertising.") (the "Cabela's Privacy Statement," collectively with the BPS Privacy Statement, the "Privacy Statements").[11]

The Privacy Statements continue, stating that each respective Defendant "ha[s] collected the following categories of information from the listed sources, used it for the listed business

[9] The version of the BPS Privacy Statement that was posted when Plaintiffs Hernandez and Cornell allege to have visited the site is archived at: https://web.archive.org/web/20220828195357/https://www.basspro.com/shop/en/privacy-policy-summary-bass-pro-shops.

[10] The version of the Cabela's Privacy Statement that was posted when Plaintiffs Montecalvo and Vonbergen allege to have visited the site is archived at: https://web.archive.org/web/20210428171300/https://www.cabelas.com/shop/en/privacy-policy-summary-cabelas.

[11] The Court can review the contents of Defendants' Privacy Statements in considering this motion because the contents of the Privacy Statements can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned and is thus subject to judicial notice. *Buck v. Hampton Twp. Sch. Dist.*, 452 F.3d 256, 260 (3d Cir. 2006); Fed. R. Evid. 201(b).

purposes and shared it with the listed categories of third parties." BPS Privacy Statement; Cabela's Privacy Statement. Within the list in the BPS Privacy Statement, BPS identifies:

Categories Of Information Collected	**Sources**	**Business Purposes* For Use**	**Categories Of Third Parties Receiving Information**
* * *			
Electronic network activity (browsing or search history, website interactions, advertisement interactions)	Information automatically collected from site visitors.	Auditing relating to transactions; security detection, protection and enforcement; functionality debugging/error repair; ad customization; performing services for you; internal research and development; quality control.	Service providers and others, such as advertising and analytics partners; affiliated companies; law enforcement.

BPS Privacy Statement.

Similarly, in the Cabela's Privacy Statement, Cabela's identifies:

Categories Of Information Collected	**Sources**	**Business Purposes* For Use**	**Categories Of Third Parties Receiving Information**
* * *			
Electronic network activity (browsing or search history, website interactions, advertisement interactions)	Information automatically collected from site visitors.	Auditing relating to transactions; security detection, protection and enforcement; functionality debugging/error repair; ad customization; performing services for you; internal research and development; quality control.	Service providers and others, such as advertising and analytics partners; affiliated companies; law enforcement.

Cabela's Privacy Statement.

Both of the Privacy Statements then go on to state that "the business purposes" for which the identified information is used, including browsing and website interactions, may include (1) "[p]erforming services" for its customers and website users; (2) "[a]dvertising customization"; (3) "[a]uditing relating to transactions, internal research and development," including "[t]o provide for internal business administration and operations, including troubleshooting, Site customization, enhancement or development, testing, research, administration and operation of our Sites and data analytics" and "[t]o measure performance of marketing initiatives, ads, and websites "powered by" another company on our behalf"; (4) "[s]ecurity detection, protection and enforcement; functionality debugging, error repair"; (5) "[d]ispute resolution"; and (6) "[q]uality control," including "[t]o develop and improve our products and services, for example, by reviewing visits to the Sites and various subpages, demand for specific products and services and user comments." BPS Privacy Statement; Cabela's Privacy Statement.

Thus, the Privacy Statements disclosed the potential collection of data associated with a website user's browsing activity and website interactions. A reasonable person browsing Defendants' website would be alerted to the Privacy Statements and their bolded provisions directly applicable to Plaintiffs' claims here. These policies appear in the homepage's footer, as they do on nearly every commercial website. Moreover, regardless of Defendants' Privacy Notices, Plaintiffs consented to the alleged capture of data here because "[a]ny reasonably intelligent person, savvy enough to be using the Internet," would be aware that to conduct an online search or click a webpage link requires her computer to send that query over the public internet to retrieve the webpage and that such transmissions "are received in a recorded format, by their very nature." *Commonwealth v. Proetto*, 771 A.2d 823, 829 (Pa. Super. 2001), *aff'd*, 837 A.2d 1163 (Pa. 2003). Likewise, to the extent Plaintiffs' Complaint is based on alleged interception of their

"communications" made in connection with their purchases, it should come as no surprise that a retailer would record those "communications" in order to maintain a record of the purchase.

In sum, Plaintiffs cannot bring a claim under any of the various wiretap statutes their Complaint relies on for conduct to which they consented. Here, at a minimum, Plaintiffs "should have known that the conversation was being recorded" *Byrd*, 235 A.3d at 319, whether because of the Privacy Notices or because of a common sense understanding of how electronic transmissions work. Plaintiffs' wiretap claims thus fail on their face because they are premised on alleged capture of information to which Plaintiffs consented. Counts I, III, VI, VIII, X, and XIII should be dismissed on this basis alone.

IV. Plaintiffs' Various Invasion of Privacy Claims (Counts VII, IX, XII, and XIV) Should be Dismissed

In addition to their wiretap claims, Plaintiffs assert a variety of common law claims for invasion of privacy and/or intrusion upon seclusion under the laws of Maryland (Count VII), Massachusetts (Count IX), Missouri (Count XII), and Pennsylvania (Count XIV).

While the formulation of the elements of these claims vary slightly, when they are applied to Plaintiffs' claims here, at their core, each state requires that Plaintiffs state: (1) an intentional intrusion by Defendants; (2) a reasonable expectation of privacy in their interactions with Defendants' website; and (3) that the intrusion into that privacy is objectionable to a reasonable person or highly offensive. *See, e.g.*, *Trundle v. Homeside Lending, Inc.*, 162 F. Supp. 2d 396, 401 (D. Md. 2001); *Polay v. McMahon*, 10 N.E.3d 1122, 1126 (Mass. 2014); *Sofka v. Thal*, 662 S.W.2d 502, 509 (Mo. 1983); *Smith v. Unilife Corp.*, 72 F. Supp. 3d 568, 574 (E.D. Pa. 2014).

Plaintiffs' invasion of privacy claims should be dismissed.[12]

[12] Plaintiffs' Pennsylvania claim (Count XIV) additionally fails because Plaintiff alleges that a right to privacy is "embodied in . . . the Pennsylvania constitution" but such a right "does not

a. Plaintiffs fail to allege an intentional intrusion.

To state a claim for intrusion upon seclusion "[i]ntent is required; the tort cannot be committed by unintended conduct amounting only to a lack of due care." *Gamble v. Fradkin & Weber, P.A.*, 846 F. Supp. 2d 377, 383 (D. Md. 2012). But an intrusion is intentional only if the defendant "believes, or is substantially certain, that she lacks the necessary legal or personal permission to commit the intrusive act." *O'Donnell v. United States*, 891 F.2d 1079, 1083 (3d Cir. 1989). Plaintiffs do not allege any such knowledge, which alone is grounds to dismiss the invasion of privacy claims. *Ruder v. Pequea Valley Sch. Dist.*, 790 F. Supp. 2d 377, 405 (E.D. Pa. 2011) (dismissing claim for failure to plead knowledge). Plaintiffs allege in a conclusory fashion that Defendants "willfully" or "intentionally" intruded on Plaintiffs' seclusion—but that allegation, alone, is not enough to support their claims. Compl. ¶¶ 280, 287, 330, 386, 393, 432. Plaintiffs must allege facts demonstrating that Defendants acted intentionally and their failure to do so requires dismissal. *See, e.g.*, *McCauley v. Suls*, 123 Md. App. 179, 190 (Md. Ct. App. 1998) (dismissing claim because the plaintiff's "bald allegations" of an intentional intrusion were "not supported by any facts pleaded in the complaint."); *Whye v. Concentra Health Servs*, 2013 WL 5375167, at *4 (D. Md. Sept. 24, 2013) *aff'd*, 583 F. App'x (4th Cir. 2014) ("the court is not required to accept legal conclusions drawn from the facts."); *see also Kurowski v. Rush Sys. for Health*, 2023 WL 2349606, at *9 (N.D. Ill. Mar. 3, 2023) (finding allegations that defendant allowed "third-party source code to collect the data [plaintiff] alleges [defendant] later disclosed" fail to state a claim for intrusion upon seclusion.

---

encompass invasions of privacy committed by *private actors*," such as Defendants. *Brooks Grp. & Assocs., Inc. v. LeVigne*, 2014 WL 1490529, at *11 & n.72 (E.D. Pa. Apr. 15, 2014).

b. Plaintiffs had no Reasonable Expectation of Privacy in Their Mouse Clicks, Mouse Movements, URLs Visited, or Keystrokes

Each of the states' laws under which Plaintiffs bring their invasion of privacy claims requires a plaintiff to have a reasonable expectation of privacy. Plaintiffs allege that they had a reasonable expectation of privacy over her alleged mouse clicks, mouse movements, URLs, and keystrokes. Compl. ¶¶ 278, 324, 384, 426. But this allegation is far from plausible, particularly because they *voluntarily* disclosed that information to Defendants. Courts have held that an intrusion upon seclusion claim requires a matter that is both "entitled to be private *and is kept private by the plaintiff*." *Neal v. United States*, 599 F. Supp. 3d 270, 306 (D. Md. 2022); *see also United States v. Bowers*, 2021 WL 2882438, at *3 (W.D. Pa. July 8, 2021) (holding no reasonable expectation of privacy in information "when a person is forewarned of the possible disclosure of the information" at issue). To the extent that Plaintiffs' website browsing constitutes communications, the communications are between Plaintiffs and Defendants themselves and were not intended to be private as to Defendants.

Nor *could* Plaintiffs allege that they have a reasonable expectation of privacy over such information—because their Complaint fails to allege that any of the data collected is *personal* to them. The Complaint discusses how session replay software *could* be configured to capture personally identifying information, (*see* Compl. ¶¶ 75-80), but fails to allege that *Defendants'* software had that capability, or even that Plaintiffs provided any personally identifying information that could be captured. To the contrary, Plaintiffs allege that Defendants' session replay software was configured to only "provide[] detailed information about website user *sessions, interactions, and engagement*, with the capacity to break down users by device type, location, and [unidentified] other dimensions"—not to collect personally identifying information. Compl. ¶ 90. As another court in this Circuit recently held, there simply is no "reasonable expectation of privacy over the

anonymized data captured by the Session Reply software" that captures "mouse movements, clicks, and keystrokes." *Massie*, 2022 WL 534468, at *2, *5 ("Plaintiffs fail to explain how either [defendant's] possession of anonymized, non-personal data regarding their browsing activities on [a defendant's] website harms their privacy interests in any way."). Courts applying the laws of the relevant jurisdictions here are in accord, limiting reasonable expectations of privacy rights to matters such as intrusions on private communications, the home, or personal movements. *See, e.g.*, *Kline v. Sec. Guards, Inc.*, 386 F.3d 246, 260 (3d Cir. 2004); *Corcoran, Corcoran, v. Southwestern Bell Tel. Co.*, 572 S.W.2d 212, 215 (Mo Ct. App. 1978) (finding opening sealed, first-class mail addressed to plaintiff was sufficient to submit to the jury); *Ruzicka Elec. and Sons, Inc. v. International Broth. Of Elec. Workers,* 427 F.3d 511, 524 (8th Cir. 2005) (holding that a "home is 'a secret and private subject matter'").

Because Plaintiffs do not have a reasonable expectation of privacy in their browsing of Defendants' websites, Counts VI, IX, XII, and XIV should be dismissed.

c. Defendants' Use of Session Replay Software is not "Objectionable to a Reasonable Person" and is Not "Highly Offensive"

Even if Plaintiffs had a reasonable expectation of privacy in their browsing data, the invasion of privacy claims still fail because Defendants' use of session replay software is not highly offensive. *Harleysville Preferred Ins. Co. v. Rams Head Savage Mill, LLC*, 237 Md. App. 705, 725 (Md. Ct. App. 2018) ("As with other privacy torts, whether conduct is 'highly offensive' is based on a test of reasonableness."); *Furman*, 744 A.2d at 586 ("Not every trespass constitutes an unreasonable search or intrusion.").

As the Third Circuit has explained in addressing technology that tracks website user activity, "the use of cookies for benign commercial purposes has become so widely accepted as part of Internet commerce that it cannot possibly be considered 'highly offensive'"—indeed,

"courts have long understood that tracking cookies can serve legitimate commercial purposes." *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 294–95 (3d Cir. 2016) (holding that the defendants' decision to use cookies was not "sufficiently offensive, standing alone, to survive a motion to dismiss"); *see also Cook*, 2023 WL 5529772 at *10 (dismissing invasion of privacy claims based on session replay technology because "the collection and disclosure of a website visitor's activity does not constitute the highly objectionable conduct needed to state a claim"); *Yook v. Lululemon USA, Inc.*, 549 F.Supp.3d 1073, 1086 (C.D. Cal. 2021) (holding that defendant's use of cookies to track users data when plaintiff was in defendant's website was not an invasion of privacy).

To state a highly offensive intrusion, far from the allegations at issue here, the invasion must be "***of the sort which would cause mental suffering, shame or humiliation to a person of ordinary sensibilities.***" *Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108, 122 (W.D. Pa. 2019) (original emphasis) (citing *Chicarella v. Passant*, 494 A.2d 1109, 1114 (1985)); *see also Axford v. TGM Andover Park, LLC*, 2021 WL 681953 (D. Mass. Feb. 22, 2021) ("Intrusion upon seclusion typically involves unwanted surveillance or other physical invasion…, unwanted contact constituting harassment …, or bodily intrusion such as drug testing."); *St. Anthony's Medical Center v. H.S.H.*, 974 S.W.2d 606, 610 (Mo. E.D. 1998) (objectionable intrusions limited to those obtained through "deception, illegal activity, or other unreasonable methods."). The allegations at issue here simply do not rise to this level. As this District explained in dismissing similar allegations in session replay litigation, "[t]he act of collecting [a website user's] keystrokes, mouse clicks, and [personal information] is simply not the type of highly offensive act to which liability can attach." *Popa*, 426 F. Supp. 3d at 122. No matter how "troubled" Plaintiffs may be by the collection of information about their purported website usage, "even well-founded concern is not

enough to give rise to tort liability." *Id.* at 123; *see also Jones v. Aberdeen Proving Ground Fed. Credit Union*, 2022 WL 1017094, at *20 (D. Md. Apr. 5, 2022) ("Conduct that a particular plaintiff finds offensive, but that would not offend a reasonable person, cannot establish intrusion upon seclusion."). Rather, "liability requires conduct that may outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities." *Popa*, 426 F. Supp. 3d at 123.

Plaintiffs baldly claim that Defendants' use of session replay software is "highly objectionable." Compl. ¶¶ 288, 331, 394, 433. But Plaintiffs fail to explain *why* this is so. And as a matter of law, it is not. The conduct alleged by Defendants in its use of session replay software—which falls short of alleging the collection of Plaintiffs' name, address, and payment information—does not rise to that level. *Popa*, 426 F. Supp. 3d at 123*; see also Nagy v. Bell Telephone Co. of PA*, 436 A.2d 701 (Pa. Super. 1981) (finding that the disclosure to an estranged husband of a list of telephone numbers called from a subscriber's telephone was not the type of highly offensive or objectionable conduct that could lead to tort liability); .

As discussed, not only did Plaintiffs voluntarily engage with Defendants' websites, but they also fails to explain how Defendants' session replay software captured any information sensitive or private to them—or anyone else for that matter. What's more, Defendants disclosed in their privacy statements that it was capturing browsing activities. *See* Section III.g, *supra*; *see also United States v. Cormack*, 2021 WL 2187016, at *10 (D. Md. May 28, 2021) (holding defendant had no reasonable expectation of privacy as to the computer based on the written warnings and the computer use policy). It is difficult to fathom how this process could "offend" anyone, let alone a reasonable person, and Plaintiffs' subjective belief that Defendants' conduct was "unreasonable" is not enough. *Popa*, 426 F. Supp. 3d at 123; *Aberdeen Proving Ground*, 2022 WL 1017094, at *20.

Counts VI, IX, XII, and XIV should all be dismissed.

V. Plaintiffs Fail to State a Claim for Violation of the Computer Fraud and Abuse Act (Count II)

Plaintiffs have not alleged facts sufficient to state a claim under the Computer Fraud and Abuse Act ("CFAA"), which was intended to combat destructive computer hacking, not to disallow standard industry session replay tools. *See Van Buren v. United States*, 141 S. Ct. 1648, 1652 (2021) (noting that the CFAA was enacted following a series of highly publicized hackings); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130 (9th Cir. 2009) ("The [CFAA] was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality[.]"); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (finding that the "legislative history supports a narrow view of the CFAA").

To bring a claim under the CFAA, plaintiffs must "plead facts that, if true, establish (1) the elements of the particular substantive (criminal) offense under subsection 1030(a); (2) the plaintiff suffered 'damage or loss' as a result of such a violation; and (3) one of the five types of conduct specified under subsection (c)(4)(A)(i)." *Pipeline Productions, Inc. v. S&A Pizza, Inc.*, 2021 WL4811206, at *5 (W.D. Mo. Oct. 14, 2021) (internal quotation omitted).

As to the first element, Plaintiffs allege that Defendants over-extended their authorization to access Plaintiffs' computer and mobile device in violation of 18 U.S.C. § 1030(a). But Defendants did not "access" Plaintiffs' computer or mobile devices. Defendants' use of session reply captured mouse movement, mouse clicks, and keystrokes on *Defendants'* website. *See, e.g.*, Compl. ¶ 99. Indeed, rather than access Plaintiffs' devices, Plaintiffs' allegations are based on Defendants tracking of their conduct on Defendants' websites. Moreover, "an individual 'exceeds authorized access' [under the CFAA] when he accesses a computer—such as files, folders, or databases—that are off limits to him." *Van Buren* 141 S.Ct. at 1662. Plaintiffs do not allege, nor

did Defendants actually, access any files, folders or databases on Plaintiffs' devices. Defendants' alleged capture of Plaintiffs' mouse movements, clicks, and keystrokes is therefore insufficient to state a claim under the CFAA.

As to the second element, "the statute defines 'damage' as 'any impairment to the integrity or availability of data, a program a system, or information.'" *Eagle v. Morgan*, 2011 WL 6739448, at *8 (E.D. Pa. Dec. 22, 2011). Courts "have held that to fall within the [CFAA definition of loss], the alleged loss must be related to the impairment or damage to a computer or computer system." *Id.; Pipeline Productions,* 2021 WL 4811206, at *5 (quoting *Burnett v. Grundy,* 2014 WL 12616808, at *2 (W.D. Mo. Oct. 28, 2014)). "Courts have interpreted the definition of damage to include the destruction, corruption, or deletion of electronic files, the physical destruction of a hard drive, or any diminution in the completeness or usability of the data on a computer system." *In re Ahern Rentals, Inc., Trade Secret Litigation*, 2021 WL 5756421, at *4 (W.D. Mo. Aug. 2021) (collecting cases) (internal quotation omitted); "Accordingly, Courts have held that merely copying data from a computer—as distinguished from damaging the data on, or removing the data from, the computer—does not constitute damage within the meaning of the [CFAA]." *Id.*

Here, Plaintiffs do not allege that their computer was impacted. Plaintiffs merely allege that their actions on Defendants' websites should not have been captured. However, capturing or copying Plaintiffs' mouse movements, clicks, keystrokes, and page visits is insufficient to constitute "damage or lost" under CFAA. *See In re Ahern Rentals, Inc., Trade Secret Litigation*, 2021 WL 5756421, at *4 ("In short, merely accessing, looking at, or copying data or information does not damage or impair the data or information"). Plaintiffs therefore do not bring a viable claim under the CFAA. Count II should be dismissed.

VI. Plaintiffs' Unfair Competition Claims Fail (Counts V and XI).

Plaintiffs Durham and Moore (on behalf of the California subclass) and Tucker (on behalf of the Missouri subclass) also bring claims under consumer protection laws of California and Missouri. Both of these claims fail.

a. California Unfair Competition Law (V)

California's Unfair Competition Law's ("UCL") prohibits any "unlawful, unfair or fraudulent business act or practice," Cal. Bus. & Prof. Code § 17200. Compl. ¶ 237. UCL provides an independent cause of action but requires an underlying violation because "[S]ection 17200 borrows violations of other laws and treats them as unlawful practices." *See Davis v. HSBC Bank*, 691 F.3d 1152, 1168 (9th Cir. 2012) (alteration in original) (quoting *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 973 P.2d 527, 539–40 (Cal. 1999)). Plaintiffs' UCL claim fails because all of their underlying claims failed.

To establish a defendant violated UCL, a plaintiff must first demonstrate UCL standing, which is distinct from Article III standing. *Mastel,* 549 F. Supp. 3d at 1144. To establish UCL standing, a plaintiff must show more than an injury in fact: she "must establish that [she] (1) suffered an injury in fact and (2) lost money or property as a result of the unfair competition." *Id.* (*citing Birdsong v. Apple, Inc.*, 590 F.3d 955, 959 (9th Cir. 2009)); *see also* Cal. Bus. & Prof. Code § 17204.

Plaintiffs have not alleged any economic injury as a result of Defendants' conduct. Plaintiffs cannot rely on "the loss of their personal information" (Compl. ¶ 245) as an economic injury. "Courts have widely held that 'personal information' does not constitute [such lost] money or property under the UCL." *Gardiner*, 2021 WL 2520103, at *8; *Rodriguez v. Google*, 2021 WL 2026726, at *8 (N.D. Cal. May 21, 2021) (individual digital data is not considered "money or

property"); *Campbell v. Facebook*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014) (misappropriation of private messages not lost "money or property").

Nor can Plaintiffs' bare allegations of "harm in the form of diminution of the value of their private and personally-identifiable data and content," Compl. ¶ 246, rescue their UCL claim, because they "do not plausibly allege that they intended to sell their . . . personal information . . . nor . . . that someone else would have bought it[.]" *Facebook Consumer Priv. Litig.*, 402 F. Supp. 3d at 784. Indeed, a California appellate court recently reaffirmed that a "lost-value-of-[personal information] theory" is "insufficient to support" standing under California's UCL where the plaintiffs "did not allege they ever attempted or intended to participate in [a] market [for their information], or otherwise to derive economic value from their" data. *Moore v. Centrelake Med. Grp., Inc.*, 83 Cal. App. 5th 515, 538 (Cal. App. Ct. 2022), review denied (Cal. Dec. 14, 2022).

Plaintiffs also cannot support a UCL claim under either the "unlawful" or "unfair" prong of the statute. Their unlawful claim is derivative of their other claims (Compl. ¶ 237) and fails for the same reasons. And Plaintiffs' assertion that Defendants' "acts and practices are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious," Compl. ¶ 244, merely recites the "South Bay test" for UCL unfairness, without any factual support. *Hodsdon v. Mars, Inc.,* 891 F.3d 857, 866 (9th Cir. 2018) (citation omitted). Such bare legal conclusions "devoid of factual support" are not enough to state a claim. *See Smith v. LG Elecs. U.S.A., Inc.,* 2014 WL 989742, at *9-10 (N.D. Cal. Mar. 11, 2014).

b. Missouri Merchandising Practices Act (XI)

To prevail on an MMPA claim, Plaintiff Tucker must demonstrate he "(1) purchased merchandise (which includes services); (2) for personal, family, or household purposes; and (3) suffered an ascertainable loss of money or property; (4) as a result of an act declared unlawful under the Merchandising Practices Act." *Murphy v. Stonewall Kitchen, LLC*, 503 S.W.3d 308, 311

(Mo. Ct. App. 2016). The Complaint fails to state a claim for at least three reasons.

i. Plaintiff Tucker does not allege a "purchase" of merchandise or service.

The MMPA gives a private right of action "only to one who *purchases* and suffers damage." *Freeman Health System v. Wass*, 124 S.W.3d 504, 506–07 (Mo. Ct. App. 2004) (emphasis supplied). "Purchase with regard to merchandise, is defined in Webster's . . . as meaning to obtain by paying money or its equivalent." *Id.* (quotation marks omitted). Here, Plaintiff Tucker does not allege that he "purchased" anything from Defendants. Absent allegations that Plaintiff Tucker made an actual purchase of merchandise, Plaintiff Tucker fails to state a claim under the MMPA. *See Raster v. Ameristar Casinos, Inc.*, 280 S.W.3d 120, 129–30 (Mo. Ct. App. 2009) (affirming a dismissal of an MMPA claim when a completed purchase was not made).

ii. Plaintiff Tucker fails to allege Defendants' supposed fraud was made "in connection with" any "merchandise."

Plaintiff Tucker's MMPA claim fails for another, independent reason. The use of an alleged unlawful practice "is a violation of the MMPA . . . *so long as it was made 'in connection with' the sale*." *Anderson v. Bass Pro Outdoor World, LLC*, 355 F. Supp. 3d 830, 836 (W.D. Mo. 2018) (emphasis in original) (quoting *Conway v. CitiMortgage, Inc.*, 438 S.W.3d 410, 414 (Mo. 2014)). The statute requires a "causal connection between the alleged violation and the transaction" because it "provides a private right of action to anyone who engages in a transaction *and thereby suffers* an ascertainable loss . . . *as a result of* a violation of the MMPA." *Anderson*, 355 F. Supp. 3d at 836 (quotation marks omitted) (citing MO. REV. STAT. § 407.025.1).

The Complaint fails to allege this causal connection. Even if Plaintiff Tucker had alleged a purchase of merchandise, the Complaint wholly lacks any factual allegations of a connection between the nonexistent purchase and Defendants' alleged fraud. Instead, Plaintiff Tucker alleges that Defendants "violated the MMPA by omitting and/or concealing material facts about" their

websites, Compl. ¶ 374, not about any merchandise for sale thereon. Specifically, Plaintiff Tucker claims that Defendants concealed that Defendants "directed Session Replay Providers to secretly monitor, collect, transmit, and disclose their . . . Website Communications to the Session Replay Providers using Session Replay Code." *Id.* These allegations do not establish a sufficient connection between Plaintiff's nonexistent transaction and an MMPA violation. *See Anderson*, 355 F. Supp. 3d at 836 (dismissing MMPA claim because "Plaintiffs generally allege that Defendant intended to increase the number of customers in its stores and on its website, and thereby increase its sales[, but] even if this is true, this does not establish a sufficient connection between Plaintiffs' transactions and the MMPA violation.").

iii. Plaintiff Tucker does not allege an "ascertainable loss."

Lastly, Plaintiff Tucker fails to allege an "ascertainable loss" as required by the MMPA. "A plaintiff adequately pleads this element of an MMPA claim if he alleges an ascertainable loss under the benefit-of-the-bargain rule, which compares the actual value of the item to the value of the item if it had been as represented at the time of the transaction." *Anderson*, 355 F. Supp. 3d at 837 (citing *Murphy v. Stonewall Kitchen, LLC*, 503 S.W.3d 308, 313 (Mo. Ct. App. 2016) and *Plubell v. Merck & Co.*, 289 S.W.3d 707, 715 (Mo. Ct. App. 2009).

Plaintiff Tucker claims he "suffered actual harm . . . because the disclosure of [his] Website Communications has value as demonstrated by the collection and use of it by Defendants." Compl. ¶ 379. This allegation does not establish an ascertainable loss. Plaintiff Tucker does not allege any purchase of merchandise, which means there is no way to calculate the benefit of the bargain he supposedly lost. Indeed, there was no "bargain" for him to benefit from at all. Plaintiff Tucker cannot allege that he failed to receive the benefit of a transaction that never occurred. *Anderson*, 355 F. Supp. 3d at 837 (W.D. Mo. 2018) (dismissing MMPA claim because the complaint did "not allege that Defendant engaged in any tactics that coerced [plaintiffs] into buying goods, or that

Defendant otherwise overbore their will. . . . [And] most importantly—Plaintiffs' argument does not establish that they failed to receive the benefit of the transactions that occurred.").

Finally, Plaintiff Tucker's MMPA claim is further deficient because it is purely speculative. Plaintiff Tucker does not allege how his website communications have value, or what that value is. Plaintiff Tucker's allegations of potential harm are not enough to establish ascertainable loss under the MMPA. *See Cregan v. Mortgage One Corporation*, 2016 WL 3072395, *4 (E.D. Mo. June 1, 2016) (citing *Roberts v. BJC Health Sys.*, 391 S.W.3d 433, 439 (Mo. 2013)) ("Potential damages are insufficient to establish an MMPA claim.").

For all these reasons, or any one of them, Plaintiff's MMPA claim should be dismissed.

VII. Plaintiffs' State Conversion and Larceny Claims Fail (Counts IV, XV, XVI)

a. Plaintiffs' Claim for Trespass and Conversion to Chattels Fail (Counts XV and XVI).

The elements of trespass to chattels and conversion are "essentially the same." *Rosemont Taxicab Co. v. Philadelphia Parking Auth.*, 327 F. Supp. 3d 803, 828 (E.D. Pa. 2018). "The difference is that conversion entails a more serious deprivation of the owner's rights such that an award of the full value of the property is appropriate." *Id.* Plaintiffs here fail to state a claim for even the less significant deprivation of an owner's rights to state a claim for trespass to chattel, much less the more extreme tort of conversion, requiring dismissal of Counts XV and XVI.

To state a viable claim for trespass to chattel, there must be an intentional intermeddling with a chattel in the possession of another that causes injury. *See Rosemont Taxicab Co. v. Philadelphia Parking Auth.*, 327 F. Supp. 3d 803, 828 (E.D. Pa. 2018); *InfoTek Corp. v. Preston*, 626 F. Supp. 3d 885, 894 (D. Md. 2022) *Foremost Ins. Co. v. Pub. Serv. Comm'n of Mo.*, 985 S.W.2d 793, 797 (Mo. Ct. App. 1998); *Best Carpet Values, Inc. v. Google LLC*, 2021 WL 4355337, at *4 (N.D. Cal. Sept. 24, 2021) (citing *Intel Corp v. Hamidi*, 30 Cal. 4th 1342, 1350-51 (2003)).

Courts have interpreted "intermeddling" to require a *physical* interference. *See e.g.*, *Rosemont*, 327 F. Supp. 3d at 828, n. 16 (quoting the Restatement (Second) of Torts § 217, cmt (E) (1965)). In other words, "there must be a disturbance of plaintiff's possession, which … may be done by an actual taking, a physical seizing …, removal from their owner, or by exercising a control or authority over them inconsistent with their owner's possession." *Pope v. Cordell*, 47 Mo. 251, 252 (1871) (citation omitted); *see also Tubbs v. Delk*, 932 S.W.2d 454, 456 (Mo. Ct. App. 1996) ("[T]o constitute trespass there must be a disturbance of plaintiff's possession, which, in the case of personal property, may be done by an actual taking, a physical seizing or taking hold of the goods, removing them from their owner, or by exercising a control or authority over them inconsistent with their owner's possession.") (quoting *Pope*, 47 Mo. at 252).

The Complaint alleges that Defendants interfered with Plaintiffs' "devices" and used or possessed the "data contained on Plaintiffs' devices." Compl. ¶¶ 444-446. As an initial matter, and as noted above, multiple courts have found that Plaintiffs' "data" is not "property." *See, e.g.*, *Gardiner*, 2021 WL 2520103, at *8. However, to the extent Plaintiffs' data even qualifies as the type of "property" that can give rise to a conversion or trespass claim, the Complaint still fails to allege that Defendants physically interfered with Plaintiffs' property. In fact, Plaintiffs merely states that the session replay "intercepted" "communications" from Plaintiffs' devices to Defendants' website. *See, e.g.*, Compl. ¶¶ 145. Plaintiffs further allege that their mouse movement, clicks, and key strokes were "recorded" from Defendants' websites via the session replay software and stored directly on Defendants' servers. *See* Compl. ¶¶ 152. But nowhere do Plaintiffs allege Defendants physically touched or possessed Plaintiffs' "devices", or "data" in any way. To the extent Plaintiffs allege their data was "stored" on Defendants' servers or in third-party cloud services, their allegations still fail. The Complaint does not allege that Plaintiffs' data was housed

anywhere that Plaintiffs had access to. Thus, there are no allegations to conclude that Plaintiffs ever "possessed" the data in order for Defendants to "seize" it. Absent plausible allegations that Defendants intermeddled with Plaintiffs' devices or data—these counts fail.

Moreover, Plaintiffs do not allege any facts that establish the requisite intent. Plaintiffs must allege that Defendants acted "for the purpose of using or otherwise intermeddling with a chattel or with knowledge that such an intermeddling will, to a substantial certainty, result from the act." *Foremost Ins. Co.*, 985 S.W.2d at 797; *see also QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 600 (E.D. Pa. 2016) (dismissing claims for conversion and trespass to chattel under Pennsylvania law for failure to allege facts supporting the requisite intent). The Complaint lacks any such allegations. To the contrary, the only purpose for Defendants' actions was that it had Plaintiffs' permission to collect any purported data at issue as discussed *supra.*

Finally, "[c]onduct which is otherwise a trespass may be justified by the fact that the intruder was authorized to do what he did." *Foremost Ins. Co.*, 985 S.W.2d at 797; *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 123 (N.D. Cal. 2020) ("a trespass only occurs where an interference is 'unauthorized'"). Plaintiffs rely on the conclusory allegation that Defendants were "unauthorized" without any additional facts or context. But as discussed above, Plaintiffs consented to the alleged recordings made by session replay software. Plaintiffs cannot now bring a claim for trespass to chattel for actions taken by Defendants that Plaintiffs consented to.

b. Plaintiffs' Statutory Larceny Claim Fails.

Plaintiffs' statutory larceny claim is inadequately pleaded, and deficient as Plaintiffs suffered no injury, and there was no intent to permanently deprive Plaintiffs of their property.

First, Plaintiffs' statutory larceny claim is subject to the heightened pleading requirements of Fed. R. Civ. P. 9(b), as it sounds in fraud. *See* Compl. ¶¶ 225-227 (alleging Defendants acted under "false pretenses," with a "false purpose," and "fraudulently appropriated"); *Kearns v. Ford*

Motor Co., 567 F.3d 1120, 1125 (9th Cir. 2009). But Plaintiffs' vague allegations that Defendants "obtained" unspecified "personal private information" (Compl. ¶ 226), does not allege any "facts constituting 'who, what, when, where, and how of the misconduct alleged," let alone any misrepresentation or malicious intent. *Kearns*, 567 F.3d at 1126; *see also Siry Investment, L.P. v. Farkhondehpour*, 513 P.3d 166, 187 (Cal. 2022) (larceny requires allegations of "criminal intent on the part of the defendant beyond mere proof of nonperformance or actual falsity").

Second, Plaintiffs fail to allege that they have loss as required for them to have statutory standing to bring a claim under § 496, which limits its cause of action to any individual "injured by a violation". Plaintiffs do not allege with any specificity that any of *their* personal information was even disclosed, but even if they had, personal information is not property so Plaintiffs' claim based on damage to a nonexistent property interest must fail. *In re Zynga Privacy Litig.*, 2011 WL 7479170, at *1 (N.D. Cal. June 15, 2011), *aff'd*, 750 F.3d 1098 (9th Cir. 2014) (in the context of a UCL claim, finding that "personally identifiable information does not constitute property").

Third, Plaintiffs do not allege an intent by Defendants to permanently deprive Plaintiffs of that property. Larceny requires, among other things, the "intent to steal the property" at issue. *Harris v. Garcia*, 734 F. Supp. 2d 973, 999 (N.D. Cal. 2010). "The intent to steal . . . is the intent . . . to permanently deprive the owner of possession." *People v. Davis*, 19 Cal. 4th 301, 305 (1998); *see also Castillo-Cruz v. Holder*, 581 F.3d 1154, 1160 (9th Cir. 2009) ("Under California law . . . § 484 requires . . . 'the specific intent to deprive the victim of his property permanently.'"). Plaintiffs do not allege that they have been permanently deprived of that information, nor would such an allegation make sense in this context.

CONCLUSION

For these reasons, Plaintiffs' Complaint should be dismissed in its entirety.

September 5, 2023

Respectfully Submitted,

By: */s/ Erin L. Leffler*

Erin (Loucks) Leffler (PA ID No. 204507)
Shook, Hardy & Bacon L.L.P.
Two Commerce Square
2001 Market St., Suite 3000
Philadelphia, PA 19103
Phone: (215) 278-2555
Fax: (215) 278-2594
eleffler@shb.com

Jennifer A. McLoone (admitted *pro hac vice*)
Shook, Hardy & Bacon L.L.P.
201 South Biscayne Boulevard
Suite 3200
Miami, FL 33131-4332
Phone: (305) 358-5171
Fax: (305) 358-7470
jmcloone@shb.com

Counsel for Defendants